CLAIMS

I/We claim:

[c1] 1. A method in a data processing system for discerning corruption of an electronic ballot, comprising:

in a voter computer system:

receiving a ballot choice selected by a voter from among a set of valid ballot choices;

encoding the received ballot choice in a ballot;

encrypting the ballot;

constructing a validity proof proving that the encrypted ballot corresponds to a valid ballot choice;

sending the encrypted ballot and the validity proof to a vote collection center computer system;

in the vote collection center computer system:

receiving the encrypted ballot and validity proof;

verifying the validity proof;

only if the validity proof is successfully verified:

without decrypting the encrypted ballot, generating an encrypted vote confirmation of the encrypted ballot;

sending the encrypted vote confirmation to the voter computer system;

in the voter computer system:

receiving the encrypted vote confirmation;

decrypting the encrypted vote confirmation to obtain a vote confirmation;

displaying the obtained vote confirmation; and

if a confirmation dictionary in the user's possession does not translate the displayed vote confirmation to the ballot choice selected by the voter, determining that the ballot has been corrupted.

[c2] 2. The method of claim 1 wherein the encoding comprises selecting a value having a predetermined correspondence to the selected ballot choice.

[c3] 3. The method of claim 1 wherein the encrypting is performed using an election public key.

[c4] 4. The method of claim 1 wherein encrypting the ballot comprises generating an *ElGamal* pair representing the ballot.

[c5] 5. The method of claim 1, further comprising signing the encrypted ballot with a private key of the voter before sending the encrypted ballot to the vote collection center computer system.

[c6] 6. The method of claim 1 wherein the vote collection center computer system sends the encrypted vote confirmation to the voter computer system via a first communication channel, further comprising, in the vote collection center computer system, sending the confirmation dictionary to the voter via a second communications channel distinct from the first communications channel.

[c7] 7. The method of claim 6 wherein the confirmation dictionary is sent in response to a request from the voter.

[c8] 8. The method of claim 7 wherein the request includes one or more identifiers associated with the voter.

[c9] 9. The method of claim 6 wherein the confirmation dictionary is sent without being requested by the voter.

[c10] 10. The method of claim 6 wherein individual confirmation dictionaries are sent to each of a plurality of voters including the voter.

[c11] 11. The method of claim 1, further comprising applying a hash function to the decrypted vote confirmation before it is displayed, and wherein it is determined that the ballot has been corrupted if the confirmation dictionary in the user's possession does not translate the displayed hashed decrypted vote confirmation to the ballot choice selected by the voter.

[c12] 12. A computer-readable medium whose content cause a data processing system to discern corruption of an electronic ballot by:

in a voter computer system:

receiving a ballot choice selected by a voter from among a set of valid ballot choices;

encoding the received ballot choice in a ballot;

encrypting the ballot;

constructing a validity proof proving that the encrypted ballot corresponds to a valid ballot choice;

sending the encrypted ballot and the validity proof to a vote collection center computer system;

in the vote collection center computer system:

receiving the encrypted ballot and validity proof;

verifying the validity proof;

only if the validity proof is successfully verified:

without decrypting the encrypted ballot, generating an encrypted vote confirmation of the encrypted ballot;

sending the encrypted vote confirmation to the voter computer system;

in the voter computer system:

receiving the encrypted vote confirmation;

decrypting the encrypted vote confirmation;

displaying the decrypted vote confirmation; and

if a confirmation dictionary in the user's possession does not translate the displayed decrypted vote confirmation to the ballot choice selected by the voter, determining that the ballot has been corrupted.

[c13] 13. A method in a data processing system for discerning corruption of an electronic ballot, comprising, in a voting node:

using a secret maintained in the voting node to encrypt a ballot value selected by a voter;

sending the encrypted ballot value to a vote collection point;

receiving, in response to sending the encrypted ballot, an encrypted vote confirmation;

using the secret maintained in the voting node to decrypt the encrypted vote confirmation; and

displaying the decrypted vote confirmation,

such that the displayed vote confirmation may be compared to an expected vote confirmation for the ballot value selected by the voter to determine whether the electronic ballot has been corrupted.

[c14] 14. The method of claim 13, further comprising:

before displaying the decrypted vote confirmation, using a hash function to transform the decrypted vote confirmation into a smaller hash output value.

[c15] 15. The method of claim 13 wherein encrypting the ballot value comprises generating an *ElGamal* pair representing the ballot value.

[c16] 16. The method of claim 15 wherein the *ElGamal* pair is generated by evaluating the expressions g^{α} and $h^{\alpha}m$, where *p* is prime; $g \in Z_p$, which has prime multiplicative order *q*, with the property that *q* is a multiplicity 1 divisor of $p - 1$; $h \in \langle g \rangle$; $\alpha \in Z_q$ is chosen randomly at the voting node; and m is the ballot value.

[c17] 17. The method of claim 15 wherein the *ElGamal* pair is generated by evaluating the expressions αg and $\alpha h + m$, where g and h are both elements of an elliptic curve group, ε, of prime order q and $\alpha \in Z_q$ is chosen randomly at the voting node, and m is the ballot value.

[c18] 18. The method of claim 13 wherein applying the secret maintained in the voting node to determine whether the encrypted vote confirmation reflects receipt of the ballot value selected by the voter at the vote collection point comprises:

determining the ballot value corresponding to the encrypted ballot value received at the vote collection point by evaluating the expression $W_i / U_i^{\alpha_i}$, where α_i is the secret maintained in the voting node, and W_i and U_i together comprise the encrypted vote confirmation; and

comparing the determined ballot value to the ballot value selected by the voter.

[c19] 19. The method of claim 13, further comprising sending to the vote collection point a validity proof proving that the encrypted ballot value corresponds to a valid ballot value.

[c20] 20. The method of claim 19 wherein the validity proof is a non-interactive proof of validity.

[c21] 21. A computer-readable medium whose contents cause a voting node to discern corruption of an electronic ballot by:

using a secret maintained in the voting node to encrypt a ballot value selected by a voter;

sending the encrypted ballot value to a vote collection point;

receiving, in response to sending the encrypted ballot, an encrypted vote confirmation; and

applying the secret maintained in the voting node to the encrypted vote confirmation to determine whether the secret value confirmation reflects receipt of the ballot value selected by the voter at the vote collection point.

[c22] 22. The computer-readable medium of claim 21 wherein the applying comprises:

using the secret maintained in the voting node to decrypt the encrypted vote confirmation; and

displaying the decrypted vote confirmation,

such that the displayed vote confirmation may be compared to an expected vote confirmation for the ballot value selected by the voter to determine whether the electronic ballot has been corrupted.

[c23] 23. The computer-readable medium of claim 21 wherein the contents of the computer-readable medium further cause the voting node to send to the vote collection point a validity proof proving that the encrypted ballot value corresponds to a valid ballot value.

[c24] 24. One or more computer memories collectively containing a voter security data structure, the data structure containing one or more secrets

usable both (a) to encrypt an encoded ballot for transmission to a ballot collection point, and (b) to decrypt an encrypted ballot confirmation received from the ballot collection point, which indicates the contents of the ballot as received at the ballot collection point.

[c25] 25. One or more computer memories collectively containing a ballot data structure, the ballot data structure comprising:

an encrypted ballot choice formed by encrypting one of a plurality of valid ballot choices selected by a voter in a voter computer system;

a proof of validity that demonstrates that the encrypted ballot choice constitutes an encryption of one of the plurality of valid ballot choices without indicating which of the plurality of valid ballot choices the encrypted ballot choice constitutes an encryption of; and

an encrypted ballot confirmation generated in response to the receipt in a ballot collection center computer system of the encrypted ballot choice and proof of validity.

[c26] 26. The computer memories of claim 25 wherein the encrypted ballot choice is an ElGamal pair.

[c27] 27. The computer memories of claim 25 wherein the memories are directly accessible by the voter computer system.

[c28] 28. The computer memories of claim 25 wherein the memories are directly accessible by the ballot collection center computer system

[c29] 29. A method in a data processing system for discerning corruption of an electronic ballot, comprising, in a ballot receiving node:

receiving an encrypted ballot value from a ballot sending node, the encrypted ballot value being encrypted from a ballot value based on a voter selection using a secret not available in the ballot receiving node;

generating from the encrypted ballot value an encrypted secret value confirmation that indicates to those in possession of the secret used to encrypt the encrypted ballot value the ballot value to which the received encrypted ballot value corresponds; and

sending the encrypted secret value confirmation to the ballot sending node,

such that the encrypted secret value confirmation may be used in the ballot sending node to determine if the encrypted ballot value received at the ballot receiving node corresponds to the ballot selection made by the voter.

[c30] 30. The method of claim 29 wherein the secret value confirmation is generated without decrypting the encrypted ballot value.

[c31] 31. The method of claim 29 wherein the secret value confirmation is sent to the ballot sending node via a first communication channel, further comprising sending to the ballot sending node a confirmation dictionary via a second communication channel distinct from the first communication channel, the confirmation dictionary translating from various possible secret value confirmations to the ballot values to which they correspond.

[c32] 32. The method of claim 29 wherein the encrypted secret value confirmation is encrypted in such a manner that, in the ballot sending node, given the encrypted secret value confirmation corresponding to a selection other than the voter selection, it is intractable to generate a decrypted secret value confirmation corresponding to the voter selection.

[c33] 33. A ballot receiving node for discerning corruption of an electronic ballot, comprising:

a receiver that receives an encrypted ballot value from a ballot sending node, the encrypted ballot value being encrypted from a ballot value derived from a selection made by a voter using a secret not available in the ballot receiving node;

a confirmation generation subsystem that generates from the encrypted ballot value an encrypted secret value confirmation that indicates to those in possession of the secret used to encrypt the encrypted ballot value the ballot value to which the received encrypted ballot value corresponds; and

a transmitter that sends the encrypted secret value confirmation to the ballot sending node.

[c34] 34. One or more generated data signals collectively conveying a ballot response data structure containing an encrypted ballot confirmation generated in response to the receipt at a ballot collection point of a ballot cast by a voter, the encrypted ballot confirmation, when decrypted on behalf of the voter, indicating a voting selection made by the voter in the cast ballot as received at the ballot collection point.

[c35] 35. The data signals of claim 34 wherein the ballot received at the ballot collection point is encrypted, and wherein the encrypted ballot confirmation is generated without decrypting the encrypted ballot.

[c36] 36. The data signals of claim 34 wherein the encrypted ballot confirmation, when decrypted, yields a value that, if the ballot received at the ballot collection point is uncorrupted, matches a value listed in a confirmation dictionary for the voting selection made by the voter.

[c37] 37. A method in a data processing system for discerning corruption of an electronic ballot, comprising:

sending an encrypted ballot from a first computer system to a second computer system, the encrypted ballot reflecting a ballot choice selected by a voter;

sending a confirmation from the second computer system to the first computer system, the confirmation serving to convey the decrypted contents of the encrypted ballot as received at the second computer system, the confirmation being generated without decrypting the encrypted ballot; and

in the first computer system, displaying the confirmation, so that the voter can determine whether the decrypted contents of the encrypted ballot as received at the second computer system match the ballot choice selected by the voter.

[c38] 38. The method of claim 37 wherein the confirmation sent from the second computer system to the first computer system is encrypted in such a manner that its decryption by the second computer system is infeasible.

[c39] 39. The method of claim 37 wherein the confirmation sent from the second computer system to the first computer system is encrypted in such a manner that its decryption by the second computer system is impossible.

[c40] 40. The method of claim 37, further comprising sending from the first computer system to the second computer system a validity proof proving that the encrypted ballot sent from the first computer system to the second computer system reflects a valid ballot choice without identifying the reflected ballot choice.

[c41] 41. The method of claim 40 wherein the confirmation is sent from the second computer system to the first computer system only if the validity proof sent from the first computer system to the second computer is verified to prove

that the encrypted ballot sent from the first computer system to the second computer system reflects a valid ballot choice.

[c42] 42. A computer-readable medium whose contents cause a data processing system to discern corruption of an electronic ballot by:

sending an encrypted ballot from a first computer system to a second computer system, the encrypted ballot reflecting a ballot choice selected by a voter;

sending a confirmation from the second computer system to the first computer system, the confirmation serving to convey the decrypted contents of the encrypted ballot as received at the second computer system, the confirmation being generated without decrypting the encrypted ballot; and

in the first computer system, displaying the confirmation, so that the voter can determine whether the decrypted contents of the encrypted ballot as received at the second computer system match the ballot choice selected by the voter.

[c43] 43. The computer-readable medium of claim 42 wherein the contents of the computer-readable medium further cause the data processing system to send from the first computer system to the second computer system a validity proof proving that the encrypted ballot sent from the first computer system to the second computer system reflects a valid ballot choice without identifying the reflected ballot choice.

[c44] 44. The computer-readable medium of claim 43 wherein the confirmation is sent from the second computer system to the first computer system only if the validity proof sent from the first computer system to the second computer is verified to prove that the encrypted ballot sent from the first computer system to the second computer system reflects a valid ballot choice.

[c45] 45. A method in a voting computing system for detecting the compromise of an electronic ballot sent to a ballot collection point, comprising:

receiving from the ballot collection point an encrypted confirmation of the contents of an encrypted ballot received at the ballot collection point; and

using a secret maintained on the voting computer system to decrypt and display the confirmation to the voter,

such that the voter may compare the displayed confirmation to a confirmation expected by the voter based on a ballot choice selected by the voter to determine whether the electronic ballot was compromised.

[c46] 46. A computer-readable medium whose contents cause a voting computing system to detect the compromise of an electronic ballot sent to a ballot collection point by:

receiving from the ballot collection point an encrypted confirmation of the contents of an encrypted ballot received at the ballot collection point; and

using a secret maintained on the voting computer system to decrypt and display the confirmation to the voter,

such that the voter may compare the displayed confirmation to a confirmation expected by the voter based on a ballot choice selected by the voter to determine whether the electronic ballot was compromised.

[c47] 47. A method in a ballot collection computer system for detecting the compromise of an electronic ballot, comprising:

receiving the electronic ballot, the electronic ballot containing an encrypted ballot choice;

determining that the received encrypted ballot choice is not accompanied by a valid validity proof that proves that the encrypted ballot choice constitutes the encryption of one of a plurality of permissible ballot choices; and

in response to so determining, determining that the generated first ballot has been compromised.

[c48] 48. The method of claim 47 wherein no validity proof is received for the encrypted ballot choice.

[c49] 49. The method of claim 47 wherein a validity proof is received along with the encrypted ballot choice, and the combination of validity proof and encrypted ballot fail a verification operation performed by the vote collection computer system,

where the verification operation is constructed explicitly to determine whether the encrypted ballot is an encryption of at least one of the valid ballot responses.

[c50] 50. A ballot collection computer system for detecting the compromise of an electronic ballot, comprising:

means for receiving the electronic ballot, the electronic ballot containing an encrypted ballot choice;

means for determining that the received encrypted ballot choice is not accompanied by a valid validity proof that proves that the encrypted ballot choice constitutes the encryption of one of a plurality of permissible ballot choices; and

means for, in response to so determining, determining that the generated first ballot has been compromised.